

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

In the Matter of the Search of
THE PREMISES LOCATED AT 4426 SHAWN DRIVE, HOUSE
SPRINGS, MO 63051.

Case No. 4:20 MJ 1229 JMB

SIGNED AND SUBMITTED TO THE COURT FOR
FILING BY RELIABLE ELECTRONIC MEANS

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the EASTERN District of MISSOURI
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENT B

YOU ARE COMMANDED to execute this warrant on or before November 2, 2020 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

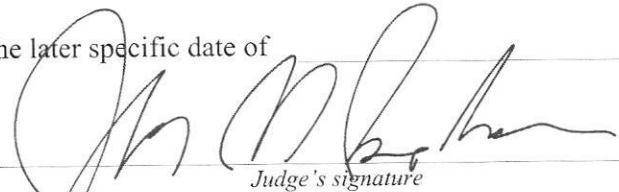
The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable John M. Bodenhausen, U.S. Magistrate Judge
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of

Date and time issued: Oct. 19, 2020 10:58 a.m.

City and state: St. Louis, MO


Judge's signature
Honorable John M. Bodenhausen, U.S. Ma
Printed name and title

 "NO KNOCK" ENTRY IS AUTHORIZED



Case No.:

Date and time warrant executed:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A

Property to be searched

The property to be searched is 4426 Shawn Dr, House Springs, MO 63051, further described as a brown and tan mobile home, to include the near-by storage shed and vehicles parked near or on the parking pad/drive way.

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. § 875, those violations involving Matthew Tilges and occurring after December 2017, including:
 - a. Records and information relating to advocating for violence and/or making threats of violence;
 - b. Records and information relating to the e-mail accounts
efguglecksckrs@gmail.com, guugleisfascistpig@gmail.com,
jackisaterrorist@protonmail.com;
 - c. Records and information relating to the identity or location of the suspects;
 - d. Records and information relating to communications with Internet Protocol addresses;
2. Computers, cellular phone, smart phone, and storage medium used as a means to commit the violations described above, including violation of 18 U.S.C. § 875.
3. For any computer, cellular phone, smart phone, or storage medium whose seizure is otherwise authorized by this warrant, and any computer, cellular phone, smart phone, or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- c. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

- i. records of or information about Internet Protocol addresses used by the COMPUTER;
 - j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
 - k. contextual information necessary to understand the evidence described in this attachment.
4. Routers, modems, and network equipment used to connect computers to the Internet.
5. Firearms, firearm magazines, ammunitions, firearm books, records, receipts, parts, notes, ledgers, and other records and equipment/tools relating to firearms.
6. Papers, tickets, notes, schedules, receipts and other items relating to travel or transportation, including, but not limited to, travel.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term “computer” includes smart phones and similar devices.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant.



IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF
THE PREMISES LOCATED AT 4426
SHAWN DRIVE, HOUSE SPRINGS, MO
63051.

No. 4:20 MJ 1229 JMB

SIGNED AND SUBMITTED TO THE
COURT FOR FILING BY RELIABLE
ELECTRONIC MEANS

FILED UNDER SEAL

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Kyle Storm, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 4426 Shawn Drive, House Springs, MO 63051, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since May 2016. I am currently assigned to the St. Louis Field Office of the FBI, assigned to full-time investigations of computer crimes with specific responsibility for criminal computer intrusions. Through my training and experience as a Special Agent, I am familiar with investigations involving individuals who execute computer intrusions, including the execution of search warrants.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Your affiant is requesting that investigators and law enforcement officers executing the requested warrant not be required to knock and announce an officer's presence. The circumstances supporting this request are described in the Probable Cause and Request for No Knock Authority sections of this affidavit.

PROBABLE CAUSE

5. A United States (US) business identified a user on their platform that was advocating for violence and making threats of violence by leaving comments on videos on their platform. The US business provided the comments to law enforcement out of a concern for life and safety of others. The person of interest made numerous directly threatening comments directed to YouTube, Google, and other social media companies. On multiple occasions, they expressed their wish to "kill every employee at google and youtube". They mentioned the CEO of YouTube Susan Wojcicki in one comment, saying "I would love to stick a sword right through susan wojicki". The person of interest made similar threatening comments towards social media companies, such as Facebook and Twitter. They made multiple threatening remarks towards Jack Dorsey, Twitter CEO, suggesting that he "must die". The person of interest's comments suggest they have access to weapons and have the means and ability to carry out the threats.

6. The person of interest used the following email addresses to create YouTube accounts. The person of interest has been using the YouTube accounts to leave publicly

available comments on various public videos on the YouTube platform. Comments left by the person of interest go back as far as Dec. 2017, starting with the efgulecksckrs@gmail.com account.

a. efgulecksckrs@gmail.com

i. Registered to YouTube Account/Channel:

UCRETu1SqE2qppkmc8wxzHpg

b. guugleisfascistpig@gmail.com

i. Registered to YouTube Account/Channel: UCnJ6-

RVdhwBClvUv68JFM_w

c. jackisaterrorist@protonmail.com

i. Registered to YouTube Account/Channel:

UCvVsmPNPM0s1ZZysxnpXNuw

7. FBI St. Louis has been investigating the user making the posts in order to determine the identity of the user. FBI St. Louis has identified the user as Matthew Thilges, 541-86-3945, DOB 06/05/1963, residing at 4426 Shawn Dr, House Spring, MO 63051, the address for which this affidavit is being sought.

Information related to account efgulecksckrs@gmail.com

8. Subscriber information related to email address, efgulecksckrs@gmail.com:

a. Name: Not a democrat

- b. Created on: February 27, 2017
- c. Creation IP address: 12.22.218.18
- d. Phone number: 636-253-9480
- e. Recovery email address: eatshitanddie@hotmail.com
- f. Registered to YouTube Channel: UCRETu1SqE2qppkmc8wxzHpg
- g. Logins:

Time	IP Address	Type
2019/05/30-01:23:11-UTC	12.139.112.194	Logout
2019/05/11-03:36:59-UTC	71.81.83.173	Login
2019/04/26-14:39:20-UTC	71.81.83.173	Logout
2019/04/26-14:38:36-UTC	71.81.83.173	Login

9. IP address 71.81.83.173, which was used to login to efguglecksckrs@gmail.com on April 26, 2019 and May 11, 2019, is an IP address assigned to Charter/Spectrum internet. Charter subscriber records for IP address 71.81.83.173 on April 26, 2019 indicate the IP address was registered to Matt Thilges, 4426 Shawn Drive, House Springs, MO 63051.

10. IP address 12.22.218.18, which was used to create the account efguglecksckrs@gmail.com, is an IP address assigned to Natoli Engineering Company since approximately November of 2015, according to a WhoIs lookup.

11. A search of employment history records for Matthew Thilges indicated that Thilges was receiving wages from Natoli Engineering Company, Inc during the quarter Jan-Mar 2017 through the quarter Apr-Jun 2018. This indicates that Thilges was employed by Natoli

Engineering Company during the time in which email address efgulecksckrs@gmail.com was created, February 27, 2017, using an IP address, 12.22.218.18, from the Natoli Engineering Company's network.

12. Phone number 636-253-9480, which is linked to efgulecksckrs@gmail.com, is linked to Matthew Thilges, DOB 06/05/1963, according to CLEAR.

13. IP address 12.139.112.194, which was used to login to efgulecksckrs@gmail.com on May 30th, 2019, is an IP address assigned to CoreLink, LLC since approximately May 2018, according to a WhoIs lookup.

14. During surveillance of Thilges on January 8, 2020, Thilges departed the residence located at 4426 Shawn Dr, House Springs, MO 63051, and proceeded to CoreLink, LLC, located at 2072 Fenton Logistics Park, Fenton, MO. Thilges drove a red Mercedes sedan bearing Missouri license TB4W7P. That vehicle is registered to Matthew Thilges, transferable upon death to Jeanette Phelps.

15. Based on the surveillance of Thilges, it is believed that Thilges likely works at CoreLink, LLC, which is where a login to efgulecksckrs@gmail.com was made on May 30th, 2019, via IP address 12.139.112.194.

Information related to account guugleisfascistpig@gmail.com

16. Subscriber information related to email address, guugleisfascistpig@gmail.com:
- a. Name: guugle/screwtube FASCISM
 - b. Created on: September 14, 2018

- c. Creation IP address: 91.219.236.171
- d. Phone number: 314-348-8345
- e. Registered to YouTube channel: UCnJ6-RVdhwBClvUv68JFM_w
- f. Logins:

Time	IP Address	Type
2018/10/29-01:53:07-UTC	75.129.194.93	Login
2018/09/15-12:54:22-UTC	47.34.97.249	Login
2018/09/14-22:54:33-UTC	91.219.236.171	Login

17. IP address 91.219.236.171 used to create guugleisfascistpig@gmail.com is a TOR node.

- a. TOR is a free and open-source software for enabling anonymous communication. The name derived from the acronym for the original software project name “The Onion Router”.

18. Phone number 314-348-8345 is registered to Jeanette Phelps. DMV records for Matthew Thilges indicates that Thilges’ vehicles are transferable upon death to Jeanette Phelps. Indicating that Thilges may have had access to Phelps phone to tie the phone number to the email account.

19. IP address 75.129.194.93, which was used to login to guugleisfascistpig@gmail.com on October 29, 2018, is an IP address assigned to Charter/Spectrum internet. Charter subscriber records for IP address 75.129.194.93 on October

29, 2018, indicate the IP address was registered to Matt Thilges, 4426 Shawn Drive, House Springs, MO 63051.

20. IP address 47.34.97.249, which was used to login to guugleisfascistpig@gmail.com on September 15, 2018, is an IP address assigned to Charter/Spectrum internet. Charter subscriber records for IP address 47.34.97.249 on September 15, 2018, indicate the IP address was registered to Matt Thilges, 4426 Shawn Drive, House Springs, MO 63051.

Information related to account jackisaterrorist@protonmail.com

21. Subscriber information related to email address, jackisaterrorist@protonmail.com:

- a. Used to register Google account 676980540741
- b. Name: Eat Shit
- c. Created on: August 26, 2019
- d. Created by IP address: 71.81.83.173
- e. Registered to YouTube channel: UCvVsmPNPM0s1ZZysxnpXNuw
- f. Logins:

+-----+-----+-----+		
Time	IP Address	Type
+-----+-----+-----+		
2020/08/28-03:30:01-UTC	71.11.249.172	Login

```
| 2020/08/01-15:35:55-UTC | 71.11.249.172 | Login |
| 2020/07/31-23:03:44-UTC | 71.11.249.172 | Login |
| 2020/07/06-08:40:20-UTC | 71.11.249.172 | Login |
| 2020/06/18-01:44:33-UTC | 71.11.249.172 | Login |
| 2020/03/11-06:45:21-UTC | 71.85.252.18 | Login |
| 2020/03/11-06:43:50-UTC | 71.85.252.18 | Logout |
| 2020/02/04-12:06:13-UTC | 144.217.80.80 | Login |
| 2020/01/17-22:39:02-UTC | 71.85.252.18 | Login |
| 2020/01/17-22:23:29-UTC | 71.85.252.18 | Logout |
| 2020/01/15-05:56:16-UTC | 71.85.252.18 | Login |
| 2020/01/15-05:55:34-UTC | 71.85.252.18 | Logout |

+-----+-----+-----+
```

22. IP address 71.81.83.173, which was used to create Google account 676980540741 on April 26, 2019 is an IP address assigned to Charter/Spectrum internet. Charter subscriber records for IP address 71.81.83.173 on April 26, 2019 indicate the IP address was registered to Matt Thilges, 4426 Shawn Drive, House Springs, MO 63051. This IP address was used to create this account and login to efguglecksckrs@gmail.com on the same date, April 26, 2019.

23. IP address 71.11.249.172, which was used to login to jackisaterrorist@protonmail.com is an IP address assigned to Charter/Spectrum internet. Charter subscriber records for the IP address indicate the IP address was registered to Matt Thilges, 4426 Shawn Dr, House Springs, MO 63051.

24. IP address 71.85.252.18, which was used to login to jackisaterrorist@protonmail.com is an IP address assigned to Charter/Spectrum internet. Charter subscriber records for the IP address indicate the IP address was registered to Matt Thilges, 4426 Shawn Dr, House Springs, MO 63051.

25. The user of the account associated with jackisaterrorist@protonmail.com continues to use the associated YouTube account to make threats of violence by commenting on publicly available YouTube videos. Below are examples of the comments being left by this user.

- a. July 8, 2020 – I do need violence. I need to kill alphabet/google/youtube employees NOW !
- b. July 8, 2020 – Todd , please name the best time and place to kill youtube employees. Asking for a friend.
- c. July 13, 2020 – Fuck the government. Kill ALL democrats. Start at alphabet/google/youtube. KILL THEM ALL !!!!!
- d. July 13, 2020 – Make the world a better place , shoot a democrat in the face. I have dibs on EVERY alphabet/google/youtube employee. You guys can start wherever you want.
- e. July 19, 2020 – “the main suspect of creating a youtube channel” , all these pigs MUST DIE. All of them. The entire department , the entire county , the entire nation. They ALL must DIE.
- f. July 22, 2020 – Kill youtube employees.

- g. July 23, 2020 – Kill youtube employees. Anywhere you can find them.
- h. July 30, 2020 – So , someone tell me where I can find them , I'll arrest them , if they resist , I'll kill them.
- i. August 15, 2020 – Make the world a better place , shoot a democrat in the face. Start with every employee of twitter , google , facebook , youtube and the main stream media. America thanks you.
- j. October 1, 2020 – If a cop , ANY cop , shows up at your door WITHOUT a warrant and attempts to KIDNAP you or any member of your family , you are not only entitled to shoot it in the face , you are OBLIGATED to do so as an American Citizen.
- k. October 4, 2020 – No more talk. Just shoot. Shoot to kill. Anywhere and everywhere. I am a staunch vehement conservative libertarian and I have absolutely had enough of government thugs and government bureaucrats. They ALL need to DIE right along with blm , antifa and EVERY member of the communist democrat party of America.
- l. October 6, 2020 – alphabet/google/youtube is a terrorist organization. Every employee must be PUT TO DEATH for sedition , subversion , insurrection , treason and crimes against humanity. The science is settled. KILL THEM ALL and DO IT NOW !

- m. October 6, 2020 – democrat children are easier to shoot than democrat “parents”.
They’re not as fast.
 - n. October 7, 2020 – If government employees murdered your business , you have
the right to murder the government employees. Call me , I will help you do that.
 - o. October 13, 2020 – Every single law abiding, tax paying citizen of the state of
Michigan now has the legal right to shoot whitmer on sight without hesitation.
The charge is treason , verdict is GUILTY.
 - p. October 13, 2020 – The harris statement at the 52 second mark grants permission
for any and every American citizen to LEGALLY kill any democrat ON SIGHT
without hesitation and without remorse.
26. Below are examples of comments left by the user of
jackisaterrorist@protonmail.com showing they have the means and ability to carry out the
threats.
- a. Approximately January of 2019 – I’ve called in for crazy shit like this while
driving twice in my life. Both times, half a dozen cop cars arrived on scene within
2 minutes. I always have 2 fully loaded semi automatic weapons in the vehicle at
all times. Never had to use them but always prepared for encounters with
democrats. St Louis County USA.
 - b. Approximately January of 2019 – Why isn’t anyone just shooting these worthless
fuckers? If I stop at an intersection and someone starts banging on my car and

screaming threats of violence, they get a bullet in the head. No hesitation and no questions asked.

- c. Approximately February of 2019 – I’ve got 6,000,000 rounds of ammo for them and anyone who supports them. That is all.

27. On October 9, 2020, a drive-by physical surveillance was conducted on Matthew Thilges’ at 4426 Shawn Drive, House Springs, MO. At approximately 9:35am, parked in the drive-way/parking pad of the residence was a black Dodge Dakota bearing Missouri license plate 8YDD45 and a red Mercedes bearing Missouri license plate TB4W7P. Thilges was observed standing at the front door of the mobile home. The mobile home is brown and tan in color with a shed near-by.

28. Based on the above information the user of the accounts, efgulecksckrs@gmail.com, guugleisfascistpig@gmail.com, and jackisaterrorist@protonmail.com, is Matthew Thilges who resides at the address 4426 Shawn Dr, House Springs, MO 63051. Thilges continues to have internet access and use electronic devices at his residence to post his threats of violence. Thilges indicates he also has the means and ability to carry out his threats through the use of firearms by shooting and killing individuals and groups. There is probable cause to believe that there is additional evidence contained in the residence related to the threats of violence related to 18 U.S.C. § 875.

TECHNICAL TERMS

29. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

30. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer, cellular phone, or smart

phone's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

31. I submit that if a computer, cellular telephone, smart phone, or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer, cellular telephone, smart phone or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer

has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

32. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the

storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used.

For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to leave comments online, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of

committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

33. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large

volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

34. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

REQUEST FOR NO KNOCK AUTHORITY

35. This affiant specifically requests that the Court authorize the executing law enforcement officers to forego the requirement to “knock-and-announce” their presence prior to making entry into the Premises. The circumstances supporting this request are described as follows. Based upon prior training and experience, investigators know that the subject of this affidavit, Matthew Thilges, has expressed threats of violence towards law enforcement and government employees. Thilges also states that he has weapons and will not hesitate to use them. As evident in the comments provided in this affidavit.

36. Based on the facts and circumstances discussed in this Affidavit, among other things, there is a significant threat to officer safety and the safety of other persons present at 4426 Shawn Dr, House Springs, MO. In other words, investigators believe that there is a substantial likelihood weapons stored at these locations and a strong potential of a violent confrontation should the search warrant team be required to knock and announce their presence at the time of the execution of the search warrant.

CONCLUSION


37. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

REQUEST FOR SEALING

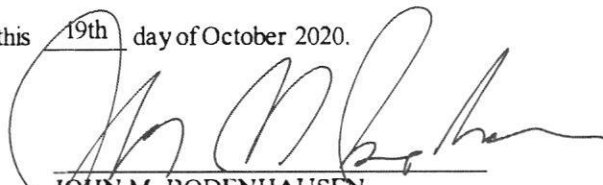
38. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and

information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

I state under the penalty of perjury that the foregoing is true and correct.


KYLE STORM
Special Agent
Federal Bureau of Investigation

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on this 19th day of October 2020.


JOHN M. BODENHAUSEN
United States Magistrate Judge

ATTACHMENT A

Property to be searched

The property to be searched is 4426 Shawn Dr, House Springs, MO 63051, further described as a brown and tan mobile home, to include the near-by storage shed and vehicles parked near or on the parking pad/drive way.

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. § 875, those violations involving Matthew Tilges and occurring after December 2017, including:
 - a. Records and information relating to advocating for violence and/or making threats of violence;
 - b. Records and information relating to the e-mail accounts efgulecksckrs@gmail.com, guugleisfascistpig@gmail.com, jackisaterrorist@protonmail.com;
 - c. Records and information relating to the identity or location of the suspects;
 - d. Records and information relating to communications with Internet Protocol addresses;
2. Computers, cellular phone, smart phone, and storage medium used as a means to commit the violations described above, including violation of 18 U.S.C. § 875.
3. For any computer, cellular phone, smart phone, or storage medium whose seizure is otherwise authorized by this warrant, and any computer, cellular phone, smart phone, or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- c. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

- i. records of or information about Internet Protocol addresses used by the COMPUTER;
 - j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
 - k. contextual information necessary to understand the evidence described in this attachment.
4. Routers, modems, and network equipment used to connect computers to the Internet.
5. Firearms, firearm magazines, ammunitions, firearm books, records, receipts, parts, notes, ledgers, and other records and equipment/tools relating to firearms.
6. Papers, tickets, notes, schedules, receipts and other items relating to travel or transportation, including, but not limited to, travel.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term “computer” includes smart phones and similar devices.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant.